



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/785,142	02/24/2004	Pierre Elie Arbajian	CHA920040006US1	8153
23550 7590 10/23/2008 HOFFMAN WARNICK LLC 75 STATE STREET 14TH FLOOR ALBANY, NY 12207				
EXAMINER				
TABOR, AMARE F				
ART UNIT		PAPER NUMBER		
2439				
NOTIFICATION DATE		DELIVERY MODE		
10/23/2008		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOCommunications@hoffmanwarnick.com

Office Action Summary

Application No.

10/785,142

Applicant(s)

ARBAJIAN, PIERRE ELIE

Examiner

AMARE TABOR

Art Unit

2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 July 2008.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-21 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 31 July 2008 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-8508)
4) ☐ Interview Summary (PTO-413)
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____
Paper No(s)/Mail Date _____

DETAILED ACTION

1. This correspondence is in response to **Amendments** and **REMARKS** filed on July 31, 2008.
2. All independent Claims [1, 12 and 17] are amended.
3. Drawing filed on 07/31/2008 [Replacement sheet for FIG.3] is considered and approved.
4. Claims 1-21 are pending.

Response to Arguments

5. Applicant's arguments with respect to the pending claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Flaherty et al. (US 6,275,824 B1 – "O'Flaherty") in view of Wong et al. (US 6,578,037 B1 – "Wong")

As per Claim 1, O'Flaherty teaches,

A data security system [see abstract], comprising: an implicit clearance system [see FIG.6; **STANDARD VIEW 260 – ROUTINE DSS APPLICATIONS 110 A** in FIG.2A; and for example, col.8, lines 16-45, "*The **standard view 260** will not present personal data unless either the flag in column 224 (indicating that the personal information and identifying information can be disseminated) or 226 (indicating that personal information can only be disseminated anonymously) is activated. Hence, the*

standard view 260 selectively masks personal data from view unless the consumer has had the appropriate flags set to the proper value...";

an explicit clearance system [see FIG.5; **METADATA MONITORING EXTENSIONS 114** in FIG.1 & FIG.5; **ACCESS LOG 402** in FIG.4; and for example, col.4, lines 37-60, "*...all access to the data stored in the extended database 106 is provided solely through the dataview suite 108... third party applications 112 have access only to such data as permitted by the database view provided... limiting access* to the data stored in the extended database 106 to access provided by the privacy dataview suite 108 for purposes of (1) implementing privacy rules provides the capability to make the personal data anonymous ... (2) to **restrict access** to opted-out columns, which can apply to all personal data, separate categories of personal data, or individual data columns, and (3) to exclude entire rows (customer records) for opt-out purposes based on customer opt-outs ..."];

a field level clearance system [see FIG.8; **PRIVILEGED VIEW 262 – PRIVILEGED APPLICATIONS 110B** in FIG.2A; and for example, col.8, line 46 to col.9, line 14, "*The **privileged view 262** permits viewing, analysis, and alteration of all information. The privileged view 262 will be supplied only to privileged ...and to those applications which handle privacy related functions ...example, the client interface module 212, which is used to view, specify, and change consumer privacy preferences, is a privileged application. Appropriate security measures are undertaken to assure that the privileged applications are suitably identified as such, and to prevent privileged view 262 access by any entity that is not so authorized...*"; and

a data anonymization system [see FIG.7; **ANONYMIZING VIEW – ANALYTICAL APPLICATIONS 110C** in FIG.2A; and for example, col.9, lines 15-54, "*The **anonymizing view 264** permits the viewing and analysis of personal information, but screens the information stored in the identity information portion 204 from view or analysis unless the flag in the column 224 ...is selected...permit data mining and ad-hoc queries. If the consumer permits, this information may also be provided to third party applications 112...*".

O'Flaherty teaches an explicit, implicit and field of clearance; but fails to teach wherein each system consists of an administrator configuration. However, in the same filed of endeavor, **Wong** discloses explicit, implicit and field of clearance systems consists of an administrator configuration [see FIG.1 – where **Wong** discloses **Database Management System 100** as an administrator configuration, including **Database Schema Object 104, Policy Group, Attribute**, etc; and for example, col.4, lines 25-47]. Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention was made, to modify the system of **O'Flaherty** by incorporating the teaching of **Wong** in order to enhance the technique for controlling access to data in a database system. The modification implements a mechanism of accessing to database that is restricted based on security policy groups selected for the user [see at least abstract of **Wong**].

As per Claim 12, O'Flaherty-Wong combination teaches,

A program product stored on a recordable medium for providing data security, the program product comprising: means for selectively requiring a user to have explicit permission in order to access a set of data [see FIG.5; **METADATA MONITORING EXTENSIONS 114** in FIG.1; **ACCESS LOG 402** in FIG.4; and for example, col.4, lines 37-60 of **O'Flaherty**];

means for requiring the user to meet any one of a set of implicit conditions in order access the set of data [see FIG.6; **STANDARD VIEW 260 – ROUTINE DSS APPLICATIONS 110 A** in FIG.2A; and for example, col.8, lines 16-45 of **O'Flaherty**];

means for limiting access to data records by restricting the user to a predefined view [see FIG.8; **PRIVILEGED VIEW 262 – PRIVILEGED APPLIACTIONS 110B** in FIG.2A of **O'Flaherty**]; and for example, col.8, line 46 to col.9, line 14, wherein the predefined view displays a predetermined set of data fields from the data records [see CUSTOMER TABLES in FIGS.2A-3C of **O'Flaherty**];

wherein the means for selectively requiring a user to have explicit permissions, the means for requiring the user to meet any one of a set of implicit conditions, and the means for limiting access to data records by restricting the user to a predefined view [see FIGS.1, 2A-3C, 4 and 8 of **O'Flaherty**] consists of an administrator configuration [see FIG.1 – where **Wong** discloses **Database Management System**

*100 as an administrator configuration; and for example, col.4, lines 25-47]; and means for replacing a data element in a data record with a unique identifier in order to create an anonymous data record [see FIG.7; **ANONYMIZING VIEW – ANALYTICAL APPLICATIONS 110C** in FIG.2A; and for example, col.9, lines 15-54 of O'Flaherty].*

As per Claim 17, O'Flaherty-Wong combination teaches,

A method for providing data security, comprising: selectively replacing data elements in data records with unique identifiers as the data records are being stored in a data warehouse in order to create anonymous data records [see FIG.7; **ANONYMIZING VIEW – ANALYTICAL APPLICATIONS 110C** in FIG.2A; and for example, col.9, lines 15-54 of O'Flaherty];

selectively requiring a user to have explicit permission in order to access a set of the data records [see FIG.5; **METADATA MONITORING EXTENSIONS 114** in FIG.1; **ACCESS LOG 402** in FIG.4; and for example, col.4, lines 37-60 of O'Flaherty] consisting of an administrator configuration [see FIG.1 – *where Wong discloses Database Management System 100 as an administrator configuration; and for example, col.4, lines 25-47];*

requiring the user to meet any one of a set of implicit conditions consisting of an administrator configuration [see FIG.1 – *where Wong discloses Database Management System 100 as an administrator configuration; and for example, col.4, lines 25-47*], in order access the set of the data records if explicit clearance is not required [see FIG.6; **STANDARD VIEW 260 – ROUTINE DSS APPLICATIONS 110 A** in FIG.2A; and for example, col.8, lines 16-45 of O'Flaherty]; and limiting access to data records by restricting the user to a predefined view [see FIG.8; **PRIVILEGED VIEW 262 – PRIVILEGED APPLICATIONS 110B** in FIG.2A; and for example, col.8, line 46 to col.9, line 14 of O'Flaherty] consisting of an administrator configuration [see FIG.1 – *where Wong discloses Database Management System 100 as an administrator configuration; and for example, col.4, lines 25-47*], wherein the predefined view displays a predetermined set of data fields from the data records [see CUSTOMER TABLES in FIGS.2A-3C of O'Flaherty].

As per Claim 2, O'Flaherty-Wong combination teaches,

wherein the implicit clearance system comprises a mechanism for setting up a plurality of filters for a set of data [see FIGS.2A-3C – *where O'Flaherty discloses plurality of filters 210, 212, SECURITY INFORMATION – CAT1, CAT2, CAT3 of O'Flaherty*], and wherein a user is granted permission to the set of data if the user meets a condition of at least one filter [see for example, col.2, lines 57-67 of **O'Flaherty**].

As per Claim 3, O'Flaherty-Wong combination teaches,

wherein the set of data is selected from the group consisting of: a row of data [see **EXTENDED-RULES-TRUSTED-ANONYMIZED DATABASE** in FIGS.1, 9 and 10 of **O'Flaherty**], a data table [see **CUSTOMER TABLES** in FIGS.2A-3C], and a data field [see **CUSTOMER BASE TABLES** in FIG.11 of **O'Flaherty**].

Claim 6 is rejected for the same reasons applied to the rejection of Claim 3.

As per Claim 4, O'Flaherty-Wong combination teaches,

wherein the implicit clearance system comprises a table for each filter, wherein each table lists all user ID's that meet the condition of an associated filter [see **CUSTOMER TABLES** in FIGS.2A-3C – *where O'Flaherty discloses ID's; e.g., ACCT NO. associated with filters 210, 212, SECURITY INFORMATION – CAT1, CAT2, CAT3 of O'Flaherty*].

As per Claim 5, O'Flaherty-Wong combination teaches,

wherein the explicit clearance system comprises a mechanism for requiring explicit permission to an area of data [see FIG.5; **METADATA MONITORING EXTENSIONS 114** in FIG.1; **ACCESS LOG 402** in FIG.4; and for example, col.4, lines 37-60 of **O'Flaherty**], and wherein a user is granted permission to the area of data only if explicit permission has been granted [see for example, col.2, lines 57-67 of **O'Flaherty**, "... a database management system, for storing and retrieving data from a plurality of database tables wherein the data in the database tables is controllably accessible according to

privacy parameters stored in the database table, ... and controlling access to the data within the database tables according to the privacy parameters, and ... for validating enforcement of the data privacy parameters in the database management system"].

As per Claim 7, O'Flaherty-Wong combination teaches,

wherein the explicit clearance system comprises: an explicit areas table that defines all areas of data that require explicit clearance [see FIG.5; **METADATA MONITORING EXTENSIONS 114** in FIG.1; **ACCESS LOG 402** in FIG.4; and for example, col.4, lines 37-60 of **O'Flaherty**]; and a set of ID tables that define those users who have explicit clearance for each of the areas requiring explicit permission [see CUSTOMER TABLES in FIGS.2A-3C of **O'Flaherty**].

Claims 13 and 18 are rejected for the same reasons applied to the rejection of Claim 7.

As per Claims 8 and 9, O'Flaherty-Wong combination teaches,

wherein the field level clearance system controls access to data types by restricting a user to a predefined view [see FIG.8; **PRIVILEGED VIEW 262 – PRIVILEGED APPLIACTIONS 110B** in FIG.2A; and for example, col.8, line 46 to col.9, line 14 of **O'Flaherty**], wherein the predefined view displays a predetermined set of data fields; and wherein the field level clearance system includes a set of data type tables that dictates data types available to each of a plurality of users [see FIGS.2A-3C of **O'Flaherty**].

As per Claims 10 and 11, O'Flaherty-Wong combination teaches,

wherein the anonymization system provides a mechanism for replacing a data element in a data record with a unique identifier in order to keep the data record anonymous; and a reference table for each data field that is to be kept anonymous, wherein each reference table includes a list of anonymized data elements and an associated unique identifier; and a mechanism for generating a new unique identifier for a data element that does not exist in the list of anonymized data elements [see **OPT-OUT VIEW 266** in FIG.2B and FIGS.3C and 11 –*where O'Flaherty discloses anonymization techniques and plurality of viewing modes*].

Claims 16 and 21 are rejected for the same reasons applied to the rejection of Claim 11.

As per Claim 14, O'Flaherty-Wong combination teaches,

wherein the means for requiring the user to meet any one of a set of implicit conditions comprises means for storing a set of acceptable user ID's for each of the implicit conditions [see CUSTOMER TABLES in FIGS.2A-3C – where O'Flaherty discloses ID's; e.g., ACCT NO. associated with filters **210, 212, SECURITY INFORMATION – CAT1, CAT2, CAT3 of O'Flaherty**].

Claim 19 is rejected for the same reasons applied to the rejection of Claim 14.

As per Claim 15, O'Flaherty-Wong combination teaches,

wherein the means for limiting access to a data record includes means for associating each of a plurality of users with one of the predefined views [see **STANDARD-PREILEGED-ANONYMIZED-OPTOUT VIEWS** in FIGS.2A-3A, 3C and 11 of **O'Flaherty**].

Claim 20 is rejected for the same reasons applied to the rejection of Claim 15.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

CONTACT INFORMATION

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2139)
/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434